LU05.A04 - Vergleich moderner symmetrischer Verschlüsselungsverfahren

Lernziele

- Ich kann moderne symmetrische Verschlüsselungsverfahren anhand von vorgegebenen Kriterien vergleichen.

Rahmenbedingungen

- **Zeitbudget:** 15 Minuten
- **Sozialform:** Einzelarbeit
- **Hilfsmittel:** Recherchen im Internet
- **Erwartetes Ergebnis:** Word-Dokument (im Vorlage im Anhang) fertig ausgefüllt

Ausgangslage

Die ersten Verschlüsselungsverfahren, wie das Skytale-Verfahren, wurden vor rund 2'000 Jahren erfunden und basierten auf einfachen Prinzipien. Im 16. Jahrhundert führte das Vigenère-Verfahren eine erhöhte Sicherheitsebene durch die Verwendung von polyalphabetischer Substitution ein, was es für damalige Verhältnisse zu einem der komplexesten Verschlüsselungsmechanismen machte. Doch mit dem Fortschritt der Kryptanalyse wurden auch diese Methoden zunehmend anfälliger für Angriffe.

Der technologische Fortschritt und das digitale Zeitalter erforderten robustere Verschlüsselungsmethoden, und so entstanden moderne symmetrische Verschlüsselungsverfahren, die auf ausgefeilten mathematischen Prinzipien beruhen. Der International Data Encryption Algorithm (IDEA) wurde als Antwort auf die Schwächen älterer Systeme entwickelt und bot eine starke Verschlüsselung mit einer Schlüssellänge von 128 Bit. Der Advanced Encryption Standard (AES) setzte später neue Maßstäbe für die Verschlüsselung von sensiblen Daten und wurde schnell zum bevorzugten Standard für Regierungen und Unternehmen weltweit. ChaCha20, eine neuere Entwicklung, ist bekannt für seine hohe Geschwindigkeit und Sicherheit, was es zu einer beliebten Wahl in modernen Protokollen wie TLS und für mobile Anwendungen macht. Von Vigenère zu IDEA, von AES zu ChaCha20, die Evolution der Verschlüsselungsmethoden spiegelt die ständige Suche nach Sicherheit in der Kommunikation wider.

Arbeitsauftrag

Recherchieren und analysieren Sie die drei modernen symmetrischen Verschlüsselungsverfahren IDEA, AES und ChaCha20. Fokussieren Sie sich auf die Kriterien Sicherheit, Schlüssellänge, bekannte Schwachstellen und praktische Anwendungsbereiche. Ermitteln Sie, wie und wo diese Algorithmen aktuell eingesetzt werden und welche Besonderheiten sie aufweisen.

Format der Tabelle

	Sicherheit	Schlüssellänge	Schwächen	Anwendungsbereiche
IDEA	...	... Bit	...	E-Mail-Verschlüsselung, VPNs, Dateiverschlüsselung
AES	...	... Bit	...	...
ChaCha20	...	... Bit	...	...

Nutzen Sie das zur Verfügung Tabellenformat, um Ihre Ergebnisse in strukturierter Form festzuhalten. Vergleichen Sie die Algorithmen miteinander und stellen Sie die gesammelten Informationen so dar, dass ein klarer Vergleich möglich ist. Achten Sie darauf, die Verwendungskontexte der einzelnen Verschlüsselungsverfahren hervorzuheben.

Solution

Lösung
